

# Tschirnhaus-Weierstrass curves

Josef Schicho and David Sevilla  
 RICAM, Austrian Academy of Sciences  
 {josef.schicho, david.sevilla}@ricam.oeaw.ac.at

## Abstract

We define the concept of Tschirnhaus-Weierstrass curve, named after the Weierstrass form of an elliptic curve and Tschirnhaus transformations. Every pointed curve has a Tschirnhaus-Weierstrass form, and this representation is unique up to a scaling of variables. This is useful for computing isomorphisms between curves.

## 1 Introduction

A elliptic curve over a characteristic zero field is given by a polynomial equation of degree 3 in two variables

$$\sum_{i+j \leq 3} a_{i,j} x^i y^j$$

that can be reduced, by invertible transformations, to the classical *Weierstrass normal form of an elliptic curve*:

$$y^2 = x^3 + ax + b$$

which characterizes the curve.

Another definition of an elliptic curve is that of a genus 1 curve. Then, the Riemann-Roch theorem [2] determines the dimensions of the Riemann-Roch spaces, from which a certain equation of degree 3 is obtained which can be simplified again. It is interesting that the generators of these spaces are then fixed up to products by constants.

Our goal in this paper is to generalize the concept of Weierstrass normal form for curves of higher genus, in such a way as to also fix the generators of the Riemann-Roch spaces up to product by constants. The interest of such property lies in the fact that it allows to improve an algorithm by F. Hess [4] for computing the set of birational isomorphisms between two given algebraic curves. (If the two curves are equal, then the result is the automorphism group; if not, then the algorithm decides whether the two curves are birationally equivalent.)

Here is a summary of the main idea of Hess's algorithm. First, pick a Weierstrass point  $P$  on the first curve (see Definition 3.4). An isomorphism has to take  $P$  to a Weierstrass point on the second curve with the same gap sequence. There are only finitely many such points, and we compute for each of them the set of isomorphisms mapping  $P$  to it. These isomorphisms induce isomorphisms on corresponding Riemann-Roch spaces, and this fact allows one to compute the isomorphisms efficiently. It is surprising that the algorithm does not use the

canonical embedding; the reason is that the embedding based on Weierstrass points leads to better complexity.

Hess's algorithm has been implemented in Magma [5], and the algorithm is quite useful for practical computations when the coefficient field is finite. Our improvement applies in the characteristic zero case. We show that the birational isomorphisms of two Tschirnhaus-Weierstrass curves mapping the unique point at infinity to the unique point at infinity can always be expressed as scalings of coordinates. The computation of these scalings is almost trivial.

As a side result, we get an easy proof for the fact that the group of birational automorphisms of a curve of positive genus fixing a point is always abelian. (This is not a new result, as it can also be obtained as a consequence of the uniformization theorem [6]).

In Section 2 we detail the elliptic curve construction and motivate our interest in fixing generators. In Section 3 we define Tschirnhaus-Weierstrass curves and show the property mentioned above in relation to maps between them.

## 2 Motivation and example

We describe in detail the construction of the equation of an elliptic curve that arises from considering the dimensions of its Riemann-Roch spaces.

**Definition 2.1.** Let  $C$  be an algebraic curve and  $P \in C$ . For any non-negative integer  $i$  we define  $\mathcal{L}(iP)$  as the vector space of all rational functions defined on  $C$  that have a pole of order  $\leq i$  at  $P$  and no other poles. This is called a *Riemann-Roch space* of  $C$  (note that the usual concept of Riemann-Roch space is defined for divisors not only of the form  $iP$ ).

**Example 2.2.** Let  $C$  be elliptic. Then  $\mathcal{L}(0) = \mathbb{C}$  and, by the Riemann-Roch theorem, for all  $i \geq 1$  and all  $P \in C$ ,  $\dim \mathcal{L}(iP) = i$ . We will now write bases of these vector spaces.

First  $\mathcal{L}(0) = \langle 1 \rangle$ . Let  $f$  be a rational function with a pole of order exactly two, then  $\mathcal{L}(2P) = \langle 1, f \rangle$ . Similarly, let  $g$  have a pole of order exactly three, then  $\mathcal{L}(3P) = \langle 1, f, g \rangle$ . Notice that, as  $\mathbb{C}(C)$  has transcendence degree one over  $\mathbb{C}$ ,  $f$  and  $g$  are algebraically dependent.

We can write further bases without introducing more functions:  $\mathcal{L}(4P) = \langle 1, f, g, f^2 \rangle$ ,  $\mathcal{L}(5P) = \langle 1, f, g, f^2, fg \rangle$ ,  $\mathcal{L}(6P) = \langle 1, f, g, f^2, fg, g^2, f^3 \rangle$ . But here we have seven elements and dimension six, so there is a non-trivial linear combination that is equal to zero:

$$a_1 + a_2f + a_3g + a_4f^2 + a_5fg + a_6g^2 + a_7f^3 = 0, \quad a_6, a_7 \neq 0. \quad (1)$$

The map  $p \mapsto (f(P), g(P))$  is birational from  $C$  to its image in  $\mathbb{C}^2$  (see Theorem 3.9). Thus, we have an equation of  $C$  in the  $(f, g)$ -plane. By performing some substitutions we can eliminate certain coefficients:

- By  $g \leftarrow g - \frac{a_5}{2a_6}f$  we can assume that  $a_5 = 0$ .
- By  $f \leftarrow f - \frac{a_4}{3a_7}$  we can assume that  $a_4 = 0$ .
- By  $g \leftarrow g - a_3/(2a_6)$  we can assume that  $a_3 = 0$ .

Note that the order is relevant since these operations change several coefficients at a time. The equation has been reduced to the classical

$$a_1 + a_2f + a_6g^2 + a_7f^3 = 0, \quad a_6, a_7 \neq 0. \quad (2)$$

**Remark 2.3.** If we substitute  $f$  or  $g$  in Equation (2) by scalar multiples of them, no new terms appear. But if we substitute  $f$  (resp.  $g$ ) by any combination  $\alpha f + \beta$ ,  $\beta \neq 0$  (resp.  $\alpha g + \beta f + \gamma$ ,  $\beta \neq 0$  or  $\gamma \neq 0$ ) then some of the terms that we eliminated appear again. In this sense, Equation (2) fixes  $f, g$  up to product by scalars.

Our interest in normal forms arises from the fact that curve isomorphisms have a particularly simple form. We illustrate this idea with the elliptic case.

**Example 2.4.** Given two elliptic curves  $C_1, C_2$  and two points  $P_1 \in C_1, P_2 \in C_2$ , we want to compute all isomorphisms  $\varphi : C_1 \rightarrow C_2$  with  $\varphi(P_1) = P_2$ . As in Example 2.2 we get:

$$\begin{aligned} a_1 + a_2f_1 + a_6g_1^2 + a_7f_1^3 &= 0 & \text{at } P_1 \\ b_1 + b_2f_2 + b_6g_2^2 + b_7f_2^3 &= 0 & \text{at } P_2 \end{aligned}$$

As  $\varphi$  induces linear isomorphisms  $\varphi^* : \mathcal{L}(iP_2) \rightarrow \mathcal{L}(iP_1)$  for all  $i$ , we have that

$$\begin{aligned} f_2 &\mapsto u_1 + u_2f_1, & u_2 &\neq 0, \\ g_2 &\mapsto u_3 + u_4f_1 + u_5g_1, & u_5 &\neq 0. \end{aligned}$$

Then we have the two equations

$$\begin{aligned} a_1 + a_2f_1 &+ a_6g_1^2 &+ a_7f_1^3 &= 0 \\ b_1 + b_2(u_1 + u_2f_1) &+ b_6(u_3 + u_4f_1 + u_5g_1)^2 &+ b_7(u_1 + u_2f_1)^3 &= 0 \end{aligned}$$

from which we get proportionality relations that imply  $u_1, u_3, u_4 = 0$ , that is,  $f_2 \mapsto u_1f_1$  and  $g_2 \mapsto u_5g_1$ , i.e. the isomorphism is an scaling in both variables.

For general curves, we will have a similar result: any isomorphism from a Tschirnhaus-Weierstrass curve (defined in the next section) to another TW curve has to be an scaling in all the variables (that is, given by a diagonal linear map). This is Theorem 4.19. The interest of such a result is in the following problem: given two curves, compute all the isomorphisms from one to the other. One solution is:

1. Compute all the Weierstrass places of both curves. There are finitely many, see Definition 3.4 and the remark preceding it.
2. Fix one Weierstrass place  $p$  in the first curve.
3. For each Weierstrass place  $q$  in the second curve, compute all the isomorphisms that send  $p$  to  $q$ .

The last step can be done efficiently thanks to the aforementioned theorem.

### 3 Weierstrass curves

In the following,  $C$  is a plane algebraic curve and  $P$  is a place of  $C$  (for example a smooth point on the curve).

**Definition 3.1.** Let  $C$  have genus  $g \geq 1$  and  $P$  be a place of  $C$ . An integer  $i \geq 1$  is called a *pole number* iff there exists a rational function over  $C$  such that its only pole is  $P$  and the order of  $P$  as a pole of  $f$  is  $i$ . Otherwise,  $i$  is called a *gap number*.

**Remark 3.2.** For any  $i \geq 1$ ,  $\dim \mathcal{L}(iP) = \dim \mathcal{L}((i-1)P) + \varepsilon$ , where  $\varepsilon$  is 1 iff  $i$  is a pole number and 0 iff  $i$  is a gap number.

**Remark 3.3.** The following are well-known facts about pole and gap numbers:

- (i) 1 is always a gap number:  $\mathcal{L}(0) = \mathbb{C}$  always, and  $L(P) = \mathbb{C}$  for any  $P$  except when  $g = 0$ .
- (ii) By Riemann-Roch,  $\dim \mathcal{L}(nP) = n + 1 - g$  for  $n \geq 2g - 1$ , so there are exactly  $g$  gap numbers at every place by Remark 3.2.
- (iii) By the previous two items, all the places of an elliptic curve have the same gap number sequence, namely 1.
- (iv) The set of pole numbers is a semigroup with respect to addition, for the product of functions with poles at  $P$  of order  $i_1$  and  $i_2$  is a function with a pole of order  $i_1 + i_2$ . It is finitely generated (this is true in general for semigroups of natural numbers, in our case it is particularly easy to prove since its complement is finite).
- (v) For a generic place of a genus  $g$  curve the gaps numbers are  $1, 2, \dots, g$ , see [1, p. 273].

**Definition 3.4.** A place in a curve of genus  $g$  is called a *Weierstrass place of the curve* iff its gap number sequence is not  $1, \dots, g$  (i.e. there is some gap number greater than  $g$ ). Note that, according to the previous remark, there are no Weierstrass places if  $g = 1$ , and places in any algebraic curve are generically non-Weierstrass.

In view of this, we introduce our main definitions.

**Definition 3.5.** Let  $C$  have only one place at infinity, and let  $f \in \mathbb{C}[C]^*$ . We define  $\deg f = -\text{ord}_\infty f$ . This is the definition of degree that we will use in the rest of the paper. We also define  $S_\infty$  as the minimal set of generators of the semigroup  $\{\deg f : f \in \mathbb{C}[C]^*\}$ .

**Definition 3.6.** A *Weierstrass curve* is a curve  $C \in \mathbb{C}^r$  such that

- (i) it has only one place at infinity,
- (ii) the function  $x_i \mapsto \deg x_i$  is a bijection between  $x_1, \dots, x_r$  and  $S_\infty$ . (alternative:  $\deg x_i = p_i, i = 1, \dots, r$ .)

**Remark 3.7.** Given a Weierstrass curve, a positive integer  $p$  is a pole number at  $\infty$  iff there exists a monomial in  $x_1, \dots, x_r$  of degree  $p$ .

**Example 3.8.** Equations (1) and (2) are Weierstrass curves, and they are birational images of the original elliptic curve, as per Theorem 3.9.

Our goal is to find Weierstrass curves of the simplest possible form that are birational to the given curve  $C$ . To this end, we will take certain Weierstrass curves that be constructed easily, and apply transformations that will cancel out some of their coefficients.

Let  $p_1, \dots, p_r$  be the minimal generators of the semigroup of pole numbers of  $P$ . If  $g > 1$ , these numbers depend on  $P$ . Let  $f_i \in \mathcal{L}(p_i P) \setminus \mathcal{L}((p_i - 1)P)$ ,  $i = 1, \dots, r$ . Note that one can choose each  $f_i$  not only up to a constant factor, but up to a linear combination of lower order functions (for methods of computing these spaces, see [3, 4]). In the next section we describe a canonical form, that we call *Tschirnhaus-Weierstrass curve*, with the property that the elements  $f_1, \dots, f_r$  are uniquely determined up to multiplication by constants.

From the  $f_i$  one can obtain equations in the fashion of Example 2.2. In relation to this, we prove now that every curve has a birational Weierstrass curve.

**Theorem 3.9.** *The rational map  $\phi : Q \mapsto (f_1(Q), \dots, f_r(Q))$  is birational.*

*Proof.* We need to show that every rational function on  $C$  can be expressed as a rational function in  $f_1, \dots, f_r$ .

Let  $g$  be a nonzero rational function on  $C$  with no poles except  $p$ . Assume that  $n$  is the pole order of  $g$  at  $P$ . Then there exists a product of  $f_1, \dots, f_r$  with exactly the same pole order. By subtracting a multiple of this product, we can reduce the pole order. This process can be repeated until the remainder is zero; this shows that  $g$  can be expressed as a polynomial in  $f_1, \dots, f_r$ .

Now, let  $h$  be an arbitrary nonzero rational function. Let  $D$  be its divisor of poles. Let  $m$  be the degree of  $D$ . Let  $l$  be a number such that  $\mathcal{L}(lP)$  has dimension bigger than  $m$ . We claim that there exists a function  $q \in \mathcal{L}(lP)$  which vanishes along  $D$ . The claim follows from the observation that vanishing along  $D$  imposes  $m$  linear conditions, and  $\dim(\mathcal{L}(lP)) > m$ . But now,  $p := hq$  has no poles other than  $P$ . Both  $p$  and  $q$  can be expressed as polynomials in  $f_1, \dots, f_r$ , hence  $h$  can be expressed as rational function in  $f_1, \dots, f_r$ .  $\square$

## 4 Tschirnhaus-Weierstrass curves

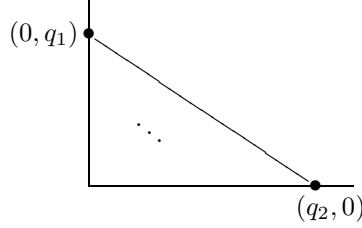
We start by constructing a Weierstrass curve in two variables and applying transformations to cancel out some of its coefficients.

Let  $p_1, p_2$  be the smallest pole generators at  $P \in C$ . We identify the functions  $f_1, f_2$  with coordinates  $x_1, x_2$ . Let  $l = \text{lcm}(p_1, p_2)$  and  $q_1 = p_1 / \text{gcd}(p_1, p_2)$ ,  $q_2 = p_2 / \text{gcd}(p_1, p_2)$ . Let  $V = \{f \in \mathbb{C}[x_1, x_2] : \deg f \leq l\}$ . Let  $A = \{0\} \cup \{\alpha p_1 + \beta p_2 \leq l : \alpha, \beta \in \mathbb{Z}^{\geq 0}\}$ . We have that  $\#A = \dim V + 1$  since there are two monomials of degree  $l$ , namely  $x_1^{q_1}$  and  $x_2^{q_2}$ . Now, let  $B$  be a set composed of one monomial  $x_1^i x_2^j$  of degree  $p$  for each  $p \in A$  and the two monomials of degree  $l$ . This set must then be linearly dependent as functions on  $C$ , so we have an equation

$$F_2 := a_1 x_1^{q_2} + a_2 x_2^{q_1} + \sum_{\substack{i,j \geq 0 \\ p_1 i + p_2 j < l}} a_{i,j} x_1^i x_2^j. \quad (3)$$

Furthermore, since the monomials  $x_1^{q_2}, x_2^{q_1}$  have the highest degree in this expression, no combination of the other monomials can be equal to only one of them (this is clear if we consider the pole orders at  $\infty$ ). Thus,  $a_1, a_2 \neq 0$ .

We have, then, that the Newton polygon of  $F_2$  is contained in the following triangle (note that the only points on the oblique edge are the two endpoints):



Let  $s := \lfloor \frac{p_2-1}{p_1} \rfloor$ . Then for any  $b, c_0, \dots, c_s$  the automorphism of  $\mathbb{C}[x_1, x_2]$  given by

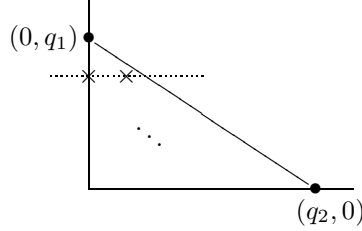
$$(x_1, x_2) \mapsto (x_1 + b, x_2 + c_0 + c_1 x_1 + \dots + c_s x_1^s) \quad (4)$$

sends  $F_2$  to another Weierstrass curve since they respect the condition on the degrees of the variables, as can be seen from the pole orders.

The classically called Tschirnhaus transformation

$$x_2 \mapsto x_2 - \frac{\sum a_{i, q_1-1} x_1^i}{a_2 q_1}$$

cancels all the terms of the form  $x_1^i x_2^{q_1-1}$ .

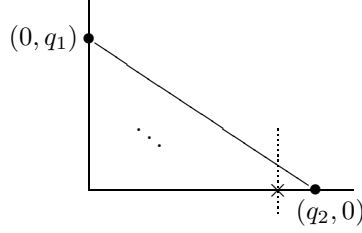


We will prove that it is an automorphism as in (4). We show that  $a_{i, q_1-1} \neq 0 \Rightarrow i \leq s$ , or equivalently  $a_{i, q_1-1} \neq 0 \Rightarrow i < q_2/q_1$ . Suppose, on the contrary, that  $a_{i, q_1-1} \neq 0$  for some  $i \geq q_2/q_1$ . If  $\alpha := i - q_2/q_1 \geq 0$ ,

$$q_1 q_2 > q_1 i + q_2(q_1 - 1) = q_1 \left( \frac{q_2}{q_1} + \alpha \right) + q_2(q_1 - 1) = q_1 q_2 + \alpha q_1$$

which is a contradiction.

Now, as  $q_1 < q_2$ , the only term  $x_1^{q_2-1} x_2^j$  that may appear is the one with  $j = 0$  (see figure below), and it can be cancelled by  $x_1 \mapsto x_1 - a_{q_2-1, 0}/a_1 q_2$ . This does not affect the coefficients made zero previously.



We have proved:

**Theorem 4.1.** *For any Weierstrass curve in two variables of the form (3) there exists an automorphism as in (4) that converts it into a Weierstrass curve with the property that all the coefficients of  $x_1^i x_2^{q_1-1}$  and the coefficient of  $x_1^{q_2-1}$  are zero.*

**Theorem 4.2.** *Let  $C_1, C_2$  be plane Weierstrass curves in the form given by Theorem 4.1. Let  $\varphi : C_1 \rightarrow C_2$  be an isomorphism. Then  $\varphi(x_1, x_2) = (\alpha_1 x_1, \alpha_2 x_2)$  for some  $\alpha_1, \alpha_2 \neq 0$ .*

*Proof.* Let  $C : F(x_1, x_2) = 0, D : G(x_1, x_2) = 0$  be Weierstrass curves satisfying the hypothesis. Then  $\varphi^* : \mathbb{C}[D] \rightarrow \mathbb{C}[C]$  preserves the degree at  $\infty$ , so the degrees of respective variables are equal. Thus  $x_1 \mapsto \alpha_1 x_1 + \beta, x_2 \mapsto \alpha_2 x_2 + \gamma_0 + \gamma_1 x_1 + \dots + \gamma_s x_1^s$  for some  $\gamma, \gamma_0, \dots, \gamma_s \in \mathbb{C}$  and  $\alpha_1, \alpha_2 \neq 0$ .

Suppose that not all the  $\gamma_i$  are zero and let  $k$  be the largest index of a nonzero  $\gamma_i$ . Substituting in  $G$  and expanding one sees that the coefficient of  $x_1^k x_2^{q_1-1}$  is nonzero, contradiction. Therefore,  $\gamma_0 = \dots = \gamma_s = 0$ . In the same way we get  $\beta = 0$  and the result is proved.  $\square$

The next step is to generalize this to Weierstrass curves with  $j \geq 3$  variables. The procedure is as follows. We construct a Weierstrass curve in  $j$  variables by finding a linear dependence among monomials in  $x_1, \dots, x_j$  which correspond to products of  $f_1, \dots, f_j$ . We choose certain monomials in it, which we can cancel out by the successive application of automorphisms  $x_j \rightarrow x_j + R(x_1, \dots, x_{j-1})$  with  $\deg R < \deg x_j$  as in Theorem 4.1, using inductively that the functions  $f_1, \dots, f_{j-1}$  have been fixed up to scalars. The induction is based on the following result.

**Theorem 4.3.** *Let  $C \subset \mathbb{C}^r$  be a Weierstrass curve and let  $\pi : C \rightarrow C' : (x_1, \dots, x_r) \mapsto (x_1, \dots, x_{r-1})$ . Then  $C'$  is again a Weierstrass curve.*

*Proof.* Let  $p_1, \dots, p_r$  be the respective degrees of the  $x_i$ . We want to show that  $\{p_1, \dots, p_{r-1}\}$  generates  $\{\deg f : f \in \mathbb{C}[C']^*\}$ . Suppose that there exists  $f \in \mathbb{C}[C']^*, f = \sum a_i m_i(x_1, \dots, x_{r-1})$  such that  $q := \deg f \notin \langle p_1, \dots, p_{r-1} \rangle_{\mathbb{Z} \geq 0}$ .

Let  $N := \{n_i\}_{i \in \langle p_1, \dots, p_{r-1} \rangle_{\mathbb{Z} \geq 0}}$  be the lexicographical normal forms in  $x_1, \dots, x_r$ ,  $\deg n_i = i$ . Then  $f$  can be written as  $\sum_{i=0}^q b_i n_i, b_q \neq 0$ . But that expression is the reduced form of  $f$  with respect to the lexicographical Gröbner basis of  $I(C)$ . By the general properties of these bases, since  $f \in \mathbb{C}[x_1, \dots, x_{r-1}] \cap I(C)$ , its reduced form does not contain  $x_r$ . In particular  $n_q$  does not involve the variable  $x_r$ , thus its degree is a combination of  $p_1, \dots, p_{r-1}$ , contradiction.  $\square$

**Remark 4.4.** One caveat in our approach is that, in general, multivariate polynomials do not allow general cancellation via Tschirnhaus transformations, the reason being that for certain exponents  $e_1, \dots, e_{j-1}$  a substitution  $x_j \leftarrow x_j + \alpha x_1^{e_1} \cdots x_{j-1}^{e_{j-1}}$  with variable  $\alpha$  may not allow us to cancel any term for any value of  $\alpha$ . But in our case, we can always obtain relations among  $f_1, \dots, f_j$  that are safe in this sense. We prove this below, first we need to introduce new concepts.

**Theorem 4.5.** *Let  $C$  be a Weierstrass curve in  $j$  variables and  $N$  be a set of monomials in  $x_1, \dots, x_j$ . The following are equivalent:*

- (i) *Every polynomial in the quotient algebra  $\mathbb{C}[x_1, \dots, x_j]/I(C)$  of  $C$  can be written uniquely as a linear combination of monomials in  $N$ .*
- (ii) *The monomials in  $N$  are a basis in the quotient algebra.*
- (iii) *The set  $N$  contains exactly one monomial of degree  $d$  for each pole number  $d$ .*

*Proof.*

(i) $\Leftrightarrow$ (ii): Obvious.

(ii) $\Rightarrow$ (iii): It is clear that there must be at least one monomial of each possible degree in  $N$ . On the other hand, if there were two monomials with the same degree, they would represent functions of the same pole order at  $\infty$ , and there would be a linear combination of lower order involving both; so it would be possible to successively lower by combining elements of  $N$  linearly. This would provide a non-trivial zero linear combination.

(iii) $\Rightarrow$ (i): A polynomial in the quotient corresponds to a function with a pole at  $\infty$  of order de degree of the polynomial. The only monomial of degree  $i$  in  $N$  also corresponds to a function with a pole of order  $i$ ; with a linear combination of both we reduce the pole order. Proceeding successively we can cancel the pole completely, and the original polynomial is expressed as a polynomial with monomials only in  $N$ .  $\square$

**Definition 4.6.** A set that satisfies the conditions in Theorem 4.5 will be called a *set of normal forms of the curve*.

**Example 4.7.** Any monomial term order based on degree, like *deglex*, determines a set of normal forms, by taking the smallest monomial of each degree.

By Theorem 4.5 and considering the relation between degrees and pole orders, it is clear that every monomial of degree less than  $p_j$  can be expressed as a linear combination of the normal forms that are smaller than  $x_j$ . Thus, we have:

**Lemma 4.8.** *Let  $N$  be a set of normal forms. Every polynomial automorphism  $x_j \rightarrow x_j + R(x_1, \dots, x_{j-1})$  with  $\deg R < \deg x_j$  can be written as a composition of substitutions  $x_j \rightarrow x_j + b_n n$ ,  $n \in N$ ,  $\deg n < \deg x_j$ .*

Our goal is to show that these substitutions can be used to cancel a coefficient of our polynomial at a time.



**Remark 4.9.** Let  $F_j$  be a polynomial in  $I \cap \mathbb{C}[x_1, \dots, x_j]$  with the following property: if the highest degree of a monomial involving  $x_j$  is  $d$ , then only one of its monomials of degree  $d$  involves  $x_j$  (we later show how to find one such polynomial). Denote this monomial as  $m = m'x_j^k$  for some  $k > 0$  and  $m' \in \mathbb{K}[x_1, \dots, x_{j-1}]$ . If we substitute  $x_j \leftarrow x_j + b_n n$  for any monomial with  $\deg n < \deg x_j$  we obtain

$$\begin{aligned} m'(x_j + b_n n)^k &= m'x_j^k + kb_n \cdot m'x_j^{k-1}n + \text{lower degree terms} \\ &= m + kb_n \cdot mn/x_j + \text{lower degree terms.} \end{aligned}$$

Now, for any other monomial  $m''x_j^{k'}, k' > 0$  of lower degree than  $m$ , by comparing degrees we can see that the same substitution cannot produce the monomial  $mn/x_j$ . Therefore, the image of  $F_j$  under this transformation differs from  $F_j$  in the coefficient of  $mn/x_j$ , which is changed linearly with respect to  $b_n$ , and in lower degree terms; thus there always exists a (unique) value of  $b_n$  that cancels the term  $mn/x_j$  and affects no higher degree monomials.

In order to construct  $F_j$ , let  $m$  be a monomial not in  $N$  involving  $x_j$ . In the quotient algebra, this monomial is equal to a nonzero linear combination of normal forms

$$m = \sum_{n \in N} a_n n.$$

One of these normal forms will have the same degree as  $m$  (in order to account for the pole order of the monomial) and the others will have smaller degree. We only need to impose that the normal form of the same degree as  $m$  does not have the variable  $x_j$ .

An additional property is desirable: since such a polynomial consists only of the monomial  $m$  and normal forms, any monomial  $mn/x_j, n \in N, \deg n < \deg x_j$  that is cancelled should also be a normal form (if not, we are just trying to kill terms that are not there in the first place).

**Definition 4.10.** Let  $N$  be a set of normal forms. A monomial  $m$  is called *good with respect to  $N$*  iff:

- (i) the element of  $N$  with the same degree as  $m$  does not involve  $x_j$ ,
- (ii)  $\forall n \in N, \deg n < \deg x_j \Rightarrow n \cdot m/x_j \in N$ .

**Remark 4.11.** (i) implies that  $m \notin N$ . (ii) is equivalent to:  $\forall n$  with  $\deg n < \deg x_j, n \in N \Rightarrow n \cdot m/x_j \in N$ .

The next algorithm describes the construction of a set of normal forms and a good monomial with respect to it.

---

**Algorithm 1:** Construct a set of normal forms and a good monomial with respect to it

---

**Input:** the degrees  $p_1, \dots, p_j$  of  $x_1, \dots, x_j$   
**Output:** a set of normal forms  $N$  and a good monomial  $m$  with respect to  $N$ . Only the normal forms of degree less than that of the good monomial are generated.

$N :=$  empty list  
**foreach** pole number  $i < p_j$  in  $\langle p_1, \dots, p_j \rangle_{\mathbb{Z} \geq 0}$  **do**  
    Compute all monomials of degree  $i$   
    Add one of them to  $N$       $/*$   
    [h]The small ones are arbitrary  
**end**  
 $s := 2p_j - p_1$   
 $found := false$   
**while**  $not(found)$  **do**  
     $s := s + 1$   
    Compute all monomials of degree  $s$   
    **if** there exist one with  $x_j$  and one without  $x_j$  **then**  
         $m :=$  one of them involving  $x_j$   
        Add one without  $x_j$  to  $N$   
         $found := true$   
    **end**  
**end**  
 $N' :=$  empty list  
**foreach**  $n$  in  $N$  **do**  
    Add  $n \cdot m/x_j$  to  $N'$   
**end**  
 $N := N \cup N'$   
**forall** pole numbers  $i$  generated by  $p_1, \dots, p_j$  only **do**  
    **if**  $i < \deg m$  and there is no monomial of degree  $i$  in  $N$  **then**  
        Compute all monomials of degree  $i$   
        Add any of them to  $N$   
    **end**  
**end**  
**return**  $N, m$

---

**Correctness proof.** The algorithm chooses the elements of the set of normal forms arbitrarily up to degree  $p_j - 1$ .

Next, a good monomial is chosen; the while loop always ends, since in particular there always exists an integer  $q \geq 2$  such that  $p_j q \in \langle p_1, \dots, p_{j-1} \rangle_{\mathbb{Z} \geq 0}$ , and then we can choose  $x_j^q$  as the good monomial (note that we can use this as a simpler way of finding a good monomial).

Then, any monomial  $m$  of sufficiently high degree will satisfy  $\deg nm/x_j > p_j$  for all  $n$  with  $\deg n < p_j$ , avoiding collisions with the already chosen normal forms. Indeed, if  $\deg m \geq 2p_j$  then  $\deg m/x_j \geq p_j$ , and for all  $n$  with  $\deg n < p_j$  we have that  $0 \leq \deg n < p_j \Rightarrow p_j \leq \deg nm/x_j < 2p_j \leq \deg m$ . In particular, none of these imposed normal forms is equal to  $m$  and we can freely choose a normal form of degree  $\deg m$  other than  $m$ , fulfilling all the conditions in Definition 4.10.

**Remark 4.12.** Now we can solve the problem posed in Remark 4.4: how to

construct from  $f_1, \dots, f_j$  a polynomial that is amenable to cancellation. Once we have computed a good monomial and normal forms with Algorithm 1, we can substitute the variables by the functions  $f_1, \dots, f_j$  in power series form, and compute explicitly a linear dependence among all the monomials. By the discussion in Remark 4.9, this is a polynomial in which we can cancel terms.

**Remark 4.13.** The definitions of good monomials, normal forms, etc. allow for very arbitrary choices. It is possible that careful choices provide better computational times, simpler equations, or other advantages. We have not investigated this; our initial approach was using the monomial orderings commonly used with Gröbner bases, but good monomials may not exist in general, due to Definition 4.10 (ii).

The result of the previous steps, that is, the construction of the  $F_j$  from a good monomial and the transformations that cancel certain terms, is what we call a Tschirnhaus-Weierstrass curve, or TW curve.

**Definition 4.14.** A *Tschirnhaus-Weierstrass curve* (abbreviated *TW curve*) is a Weierstrass curve  $C \subset \mathbb{C}^r$  together with pairs  $\{(N_j, m_j)\}_{j=2, \dots, r}$  such that, for every  $j$ :

- $N_j$  is a set of normal forms in  $x_1, \dots, x_j$  for the projection of  $C$  onto those variables;
- $m_j$  is a good monomial with respect to  $N_j$ ;
- the polynomial  $F_j(x_1, \dots, x_j) := m_j - \sum_{n \in N_j} a_{j,n} n$  defined uniquely by the condition  $F_j \in I(C)$  has the property that all the monomials of the form  $n \cdot m_j / x_j$ ,  $n \in N_j$ ,  $\deg n < \deg x_j$ , have coefficient zero.

Informally, a TW curve is a collection of polynomials  $P_j(x_1, \dots, x_j)$ ,  $j = 2, \dots, r$  satisfying the conditions of cancellation described previously.

**Example 4.15.** All Weierstrass curves in the form given in Theorem 4.1 are in Tschirnhaus-Weierstrass form.

The algorithm that we describe now uses the ideas above to compute a TW curve birational to a given one.

---

**Algorithm 2:** Compute a TW curve birational to a given curve

---

**Input:** a plane curve  $C$  and a place  $P$  of  $C$

**Output:** an integer  $r$ , a birational morphism  $C \hookrightarrow \mathbb{C}^r$  to a TW curve and a list of equations of the image

Compute the pole generators  $p_1, \dots, p_r$  at  $P$

Compute functions  $f_1, \dots, f_r$  with pole orders the  $p_i$

**for**  $j$  from 2 to  $r$  **do**

$m_j, N_j :=$  good monomial and normal forms for  $x_1, \dots, x_j$  (Alg 1)

Compute a linear dependence among them:  $P_j(f_1, \dots, f_j) = 0$

**for**  $k \in \langle p_1, \dots, p_{j-1} \rangle_{\mathbb{Z} \geq 0}$ ,  $k < p_j$  in decreasing order **do**

Find  $\alpha$  such that  $f_j \leftarrow f_j + \alpha n_k$  cancels the term  $n_k f_j^{q_j-1}$  in  $P_j$

Substitute  $f_j \leftarrow f_j + \alpha n_k$  and apply this to  $P_j$

**end**

**end**

**return**  $r, (f_1, \dots, f_r), [P_2, \dots, P_r]$

---

**Correctness proof.** In each run of the main loop an equation in the first  $j$  variables (or functions) is computed. This is done by choosing normal forms and good monomials in a similar way to Algorithm 1. In this way it is ensured that for each substitution a coefficient  $\alpha$  exists that will kill a corresponding monomial in the equation, since the resulting equation for  $\alpha$  is linear (see Remark 4.9). Therefore the output matches the conditions in Definition 4.14.

**Example 4.16.** The curve  $C : x - y^2 + x^2 y^2 + y^4 = 0$  is hyperelliptic of genus 2, its Weierstrass places being the six points  $(-2\gamma^4 + 2\gamma^2, \gamma)$  with  $4\gamma^6 - 4\gamma^4 - 1 = 0$ . By Remark 3.3 the gap numbers at these six points are 1, 3 and the gap numbers at any other point are 1, 2. In the first case the pole generators are 2, 5 so the computation of a TW form is entirely similar to Example 2.2. The other case has pole generators 3, 4, 5, we compute a TW form for the point  $P = (0, 0)$ .

First we compute an equation in  $x_1, x_2$ . Following the construction at the beginning of Section 4 we have  $q_1 = 3, q_2 = 4$  and we will get a degree 12 polynomial. Let us show in any case a table of relevant monomials, excluding the constant.

deg	monomials	deg	monomials
3	$x_1$	8	$x_2^2$
4	$x_2$	9	$x_1^3$
5	$x_3$	10	$x_1^2 x_2$
6	$x_1^2$	11	$x_1 x_2^2$
7	$x_1 x_2$	12	$x_1^4, x_2^3$

In any case there is a polynomial equation

$$F_2 := a_1 x_1^4 + a_2 x_2^3 + \sum_{3i+4j < 12} a_{i,j} x_1^i x_2^j = 0.$$

We compute its coefficients by means of the associated functions  $f_1 = (y^2 - 1)/xy$  and  $f_2 = (x - 1 + y^2)/x^2$  and the Puiseux expansion at  $P$

$$x = T^2, \quad y = T + \frac{1}{2}T^3 + \frac{11}{8}T^5 + \dots$$

We obtain

$$F_2(x_1, x_2) = x_1^4 + x_2^3 + 2x_2^2 + x_1^2 + x_2.$$

The substitution  $x_2 \mapsto x_2 - 2/3$  kills the term  $2x_2^2$  and the new polynomial

$$x_1^4 + x_2^3 + x_1^2 - \frac{1}{3}x_2 - \frac{2}{27}$$

satisfies the TW condition. Now we have  $f_1$  as before and  $f_2 = (x - 1 + y^2)/x^2 + 2/3$ .

The next step is to compute an equation involving  $x_1, x_2, x_3$ . Here are the first monomials.

deg	monomials	deg	monomials
3	$x_1$	6	$x_1^2$
4	$x_2$	7	$x_1 x_2$
5	$x_3$	8	$x_1 x_3, x_2^2$

The monomial  $x_1 x_3$  is a good monomial if we take all the other monomials in the table as normal forms. Indeed, the condition in this case is that  $1, x_1, x_2 \in N \Rightarrow x_1, x_1^2, x_1 x_2 \in N$  which is trivially true since there are no other candidates.

This gives

$$F_3 := b_1x_1x_3 + b_2x_2^2 + b_3x_1x_2 + b_4x_1^2 + b_5x_3 + b_6x_2 + b_7x_1 + b_8 = 0.$$

Using the  $f_1, f_2, f_3 := (-x^2 + 4y^2x - 4y^2 + 4y^4)/4x^3y$  we compute

$$F_3(x_1, x_2, x_3) = x_1x_3 - x_2^2 + x_1^2 + \frac{1}{3}x_2 + \frac{2}{9}.$$

Now, two of the three target monomials do not appear in  $F_3$  and we can kill  $x_1^2$  with  $x_3 \mapsto x_3 - x_1$  so that  $f_3$  becomes  $f_3 + f_1$  and  $F_3$  becomes

$$x_1x_3 - x_2^2 + \frac{1}{3}x_2 + \frac{2}{9}.$$

Thus, the map  $(x, y) \mapsto (f_3(x, y), f_4(x, y), f_5(x, y))$  is birational onto its image  $C' = V(F_2, F_3)$ .

If we want to compute the automorphisms of the original curve that send  $(0, 0)$  to itself, we look for automorphisms  $(x_1, x_2, x_3) \mapsto (\alpha_1x_1, \alpha_2x_2, \alpha_3x_3)$  of the image curve. From  $F_2$  we get  $\alpha_1^2 = 1, \alpha_2 = \alpha_3 = 1$  and from  $F_3$  we get  $\alpha_1\alpha_3 = 1, \alpha_2 = 1$  so that the only automorphism is the identity.

**Remark 4.17.** It is possible to choose the normal forms incrementally, that is, a normal form chosen in a certain step is also a normal form in subsequent steps. This certainly simplifies the output, since the set of normal forms for  $x_1, \dots, x_j$  is just the intersection of the biggest set of normal forms with  $\mathbb{C}[x_1, \dots, x_j]$ .

**Remark 4.18.** There is another method of computing a TW curve, besides direct manipulation of the  $f_j$  and the resulting equations among them as in Algorithm 2. It consists of implicitizing the image curve given by the initial  $f_1, \dots, f_r$  and then compute polynomials in less variables in the ideal of that curve that satisfy the condition in Remark 4.9. This approach requires computation of Gröbner bases, so we have preferred to describe the more direct procedure in the main section.

As we said previously, our motivation is the computation of isomorphisms of curves. This is the main result.

**Theorem 4.19.** *Let  $C_1, C_2$  be TW curves with the same normal forms and good monomials. If  $\varphi : C_1 \rightarrow C_2$  is an isomorphism, it is given by a diagonal matrix. (i.e.  $\varphi(x_1, \dots, x_r) = (y_1, \dots, y_r)$  with  $y_i = \lambda_i x_i$ .)*

*Proof.* Let  $x_1, \dots, x_r$  and  $y_1, \dots, y_r$  be coordinates for  $\phi_1, \phi_2$  with increasing degrees.

We will prove the result by induction on  $j$ . The base case  $j = 2$  is Theorem 4.2. So assume without loss of generality that  $\varphi^*(y_i) = \lambda_i x_i$  for  $i = 1, \dots, j-1$ .  $\varphi$  induces an isomorphism  $\varphi^* : \mathcal{L}(p_j P_2) \rightarrow \mathcal{L}(p_j P_1)$ , thus  $\varphi^*(y_j) \in \mathcal{L}(p_j P_1)$ , so

$$\varphi^*(y_j) = \lambda_j x_j + \sum_{\substack{n \in N_j \\ n < x_j}} \alpha_n \cdot n$$

and we can assume without loss of generality that  $\lambda_j = 1$ . Our goal is to prove that all the  $\alpha_n$  are zero. Suppose the contrary and let  $n \in N_j, n < x_j$  be the

largest monomial with  $\alpha_n \neq 0$ . Let  $m_1, m_2$  be the good monomials for  $x_j, y_j$  respectively.

For any monomial  $t$  in the  $x$ 's (resp.  $y$ 's) we call  $r(t)$  the only linear combination of normal forms in the  $x$ 's (resp.  $y$ 's) that is equal to  $t$  in the quotient algebra of  $C_1$  (resp.  $C_2$ ).

Let  $G_1 := m_1 - r(m_1) \in I(C_1)$ ,  $G_2 := m_2 - r(m_2) \in I(C_2)$ . Let  $G_3 := \varphi^*(G_2) - m_1$ . Since  $G_3 - r(G_3)$  and  $\varphi^*(G_2) = m_1 + G_3$  both belong to  $I(C_1)$ , we have that  $m_1 + r(G_3) \in I(C_1)$  too. But  $G_1$  is the only polynomial in  $I(C_1)$  of the form  $m_1$ +normal forms, therefore  $m_1 + r(G_3) = G_1$ .

By the computation in Remark 4.9, the leading term of  $G_3$  is  $k\alpha_n \cdot m_1 n / x_j$ , where  $k > 0$  is the exponent of  $x_j$  in the good monomial  $m_1$ . But, by definition of TW curve, this term has coefficient zero in  $G_1$ , therefore  $\alpha_n = 0$ , which contradicts our previous assumption.  $\square$

## References

- [1] P. Griffiths, J. Harris, *Principles of algebraic geometry*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York, 1978. xii+813 pp. ISBN: 0-471-32792-1.
- [2] R. Hartshorne, *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. ISBN: 0-387-90244-9.
- [3] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*. J. Symbolic Comput. 33 (2002), no. 4, 425–445.
- [4] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*. In *Algorithmic number theory*, 263–271, Lecture Notes in Comput. Sci., 3076, Springer, Berlin.
- [5] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* 24 (1997), no. 3-4, 235–265.
- [6] H. Weyl, *Die Idee der Riemannschen Fläche. (German) [The concept of a Riemann surface]* Reprint of the 1913 German original. With essays by Reinhold Remmert, Michael Schneider, Stefan Hildebrandt, Klaus Hulek and Samuel Patterson. Edited and with a preface and a biography of Weyl by Remmert. Teubner-Archiv zur Mathematik. Supplement [Teubner Archive on Mathematics. Supplement], 5. B. G. Teubner Verlagsgesellschaft mbH, Stuttgart, 1997. xxii+240 pp. ISBN: 3-8154-2096-2.